# A Method To Find Quantum Noiseless Subsystems

Man-Duen Choi[1] and David W. Kribs[2,3]

[1]*Department of Mathematics, University of Toronto, ON Canada, M5S 3G3*
[2]*Department of Mathematics and Statistics, University of Guelph, Guelph, ON, Canada, N1G 2W1*
[3]*Institute for Quantum Computing, University of Waterloo, ON Canada, N2L 3G1*

(Dated: February 1, 2008)

We develop a structure theory for *decoherence-free subspaces* and *noiseless subsystems* that applies to arbitrary (not necessarily unital) quantum operations. The theory can be alternatively phrased in terms of the superoperator perspective, or the algebraic noise commutant formalism. As an application, we propose a method for finding all such subspaces and subsystems for arbitrary quantum operations. We suggest that this work brings the fundamental passive technique for error correction in quantum computing an important step closer to practical realization.

PACS numbers: 03.67.Pp, 03.67.Hk, 03.67.Lx



*Introduction.* — The problem of controlling and maintaining properties of quantum systems which are in contact with an environment has received considerable recent attention. Primarily these investigations have been driven by the need to better understand the special features of evolving quantum systems that distinguish the quantum computing paradigm. Of central importance in the field of "quantum error correction" is the requirement for techniques to avoid and overcome the degrading effects of decoherence. Early work in quantum error correction included the realization that many physical error models contain symmetries induced by the system-environment interplay. This led to the discovery of "decoherence-free subspaces" (DFS) and "noiseless subsystems" (NS) [1, 2, 3, 4, 5, 6, 7]. (On occasion we shall refer to both notions jointly as "NS".) In these schemes, subspaces – and subsystems in the more abstract case – are identified within a system Hilbert space, with the property that all initial states encoded therein remain immune to the errors of a quantum operation of interest. Experimental efforts [8, 9, 10, 11] have affirmed the viability of this "passive quantum error correction" (PQEC) technique.

It is also becoming clear that the NS formalism is applicable beyond the realm of quantum error correction. In quantum communication and cryptography, for instance, NS have been used as vehicles for avoiding noise [12]; this may lead to practical applications of NS in the near future. Further, NS are ideal for determining how to achieve distributed quantum information processing in the absence of shared reference frames [13]. The NS concept has also arisen in recent analysis of black holes [14], and quantum gravity [15], where NS are used to identify the relational symmetry-invariant physical degrees of freedom in the quantum causal history framework.

There is an obvious advantage to PQEC in the context of quantum computing. If a quantum operation (or channel) is found to possess NS, then, by taking care at the initial encoding stage, the need for active error correction after the fact is minimized. However, this protocol has a notable drawback. While substantial analysis has been carried out in important special cases, the protocol lacks a general method to find NS for arbitrary quantum operations. It is our belief that the PQEC approach will play a substantive role in quantum computing devices, and in applications beyond quantum computing, only if some sort of general approach for finding NS is derived.

In this paper we propose such a method. Specifically, we develop a structure theory that shows precisely how properties of a quantum operation as a superoperator determine its NS structure. Moreover, if an operator-sum decomposition of Kraus (or "error") operators $\mathcal{E} = \{E_a\}$ for a channel $\mathcal{E}$ is known, we show how algebraic properties of the operators $E_a$ determine this structure. This information naturally leads to the aforementioned method. Our analysis utilizes the framework for NS recently introduced under the umbrella of "operator quantum error correction" in [16, 17] (see also [18]).

As a consequence of this work, we suggest that the fundamental passive technique for error correction in quantum computing has been brought an important step closer to practical realization. Let us discuss these points further through a pair of illustrative examples, full details of the theory will be provided below.

First we consider a simple example. Let $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$ be the combined system Hilbert space for two spin-$\frac{1}{2}$ particles. Let $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ be the associated basis. Consider the channel $\mathcal{E} = \{Z_1, Z_2\}$ where $Z_1 = Z \otimes \mathbb{1}_2$ and $Z_2 = \mathbb{1}_2 \otimes Z$, with the Pauli matrix $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$. Then the action of $\mathcal{E}$ on a density matrix $\rho$ on $\mathcal{H}$ is given by $\mathcal{E}(\rho) = \frac{1}{2}(Z_1 \rho Z_1^\dagger + Z_2 \rho Z_2^\dagger)$. This channel has no nontrivial NS. The key point is that the "noise commutant" $\mathcal{A}' = \{Z_1, Z_2\}'$, which is the set of all operators on $\mathcal{H}$ that commute with both $Z_1$ and $Z_2$, only contains the diagonal matrices with respect to the standard basis; i.e., the matrices corresponding to classical states. On the other hand, suppose our channel is $\mathcal{F} = \{U_1, U_2\}$, where $U_k = UZ_k$, $k = 1, 2$, and $U = \mathbb{1}_4 - 2\,|11\rangle\langle 11|$. In this case, the noise commutant $\mathcal{A}' = \{U_1, U_2\}'$ contains a single qubit NS (in fact it is a DFS). Indeed, any operator of

the form $\sigma = a|00\rangle\langle 00| + b|00\rangle\langle 11| + c|00\rangle\langle 11| + d|11\rangle\langle 11|$, $a, b, c, d \in \mathbb{C}$, belongs to $\mathcal{A}'$ and satisfies $\mathcal{E}(\sigma) = \sigma$. As discussed below, that this NS is also fixed by $\mathcal{E}$ follows from the fact that $\mathcal{E}$ is unital, or bistochastic; i.e., $\mathcal{E}(\mathbb{1}) = \mathbb{1}$.

As a new example of NS, and one that will also be discussed further below, we consider an error model first discussed in [19] in the context of active error correction. In this case the channel $\mathcal{E} = \{E_0, E_1, E_2\}$ acts on 2-qubit space and has three Kraus operators given by

$$E_0 = \alpha(|00\rangle\langle 00| + |11\rangle\langle 11|) + |01\rangle\langle 01| + |10\rangle\langle 10|, \quad (1)$$
$$E_1 = \beta(|00\rangle\langle 00| + |10\rangle\langle 00| + |01\rangle\langle 11| + |11\rangle\langle 11|), \quad (2)$$
$$E_2 = \beta(|00\rangle\langle 00| - |10\rangle\langle 00| - |01\rangle\langle 11| + |11\rangle\langle 11|), \quad (3)$$

where $q$ is a scalar $0 < q < 1$ with $\alpha = \sqrt{1-2q}$ and $\beta = \sqrt{q/2}$. One can check that $\mathcal{E}(\mathbb{1}) = \sum_{i=0}^{2} E_i E_i^\dagger \neq \mathbb{1}$, and hence $\mathcal{E}$ is non-unital. As we show below, the noise commutant here $\mathcal{A}' = \{E_0, E_1, E_2\}'$ supports a single qubit NS that is not fixed by the action of $\mathcal{E}$. Further, there is another NS for the channel, in fact a DFS, that is not contained in the noise commutant. In particular, if we define the projector $P = |01\rangle\langle 01| + |10\rangle\langle 10|$, then all operators supported by $P$ are fixed by $\mathcal{E}$; that is, $\mathcal{E}(\sigma) = \sigma$ for all $\sigma = P\sigma P$. However, these operators do not belong to the noise commutant. For instance, notice that $E_i P = 0 \neq PE_i$ for $i = 1, 2$. Hence, this error model has a NS inside its noise commutant that is not fixed, and a fixed DFS that is not contained in its noise commutant.

Thus, one can ask, what is the underlying phenomena that produces noiseless subsystems? The previous example indicates that we must consider more than the noise commutant and fixed point set for the map. As it turns out, the structure theory we derive for NS can be phrased in terms of more general operator algebras obtained in the same spirit as the noise commutant, and, alternatively, in terms of modified fixed point sets for the map. Therefore, our approach has the advantage of either being set in an algebraic context, or strictly in terms of properties of the superoperator.

The rest of the paper is organized as follows. We next recall the NS framework. We follow this by proving a theorem that yields the structure theory, and then show precisely how it may be used to find NS. Optimality of the method is then established, and this is followed with a conclusion on possible future work and limitations.

*Noiseless Subsystem Framework.* — Given a quantum operation (or "channel"), represented by a completely positive, trace preserving superoperator $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ on a (finite dimensional) Hilbert space $\mathcal{H}$, the NS protocol [1, 2, 3, 4, 5, 6, 7, 16, 17] seeks subsystems $\mathcal{H}^B$ (with $\dim \mathcal{H}^B > 1$) of the full system Hilbert space $\mathcal{H} = (\mathcal{H}^A \otimes \mathcal{H}^B) \oplus \mathcal{K}$ such that

$$\forall \sigma^A \ \forall \sigma^B, \ \exists \tau^A \ : \ \mathcal{E}(\sigma^A \otimes \sigma^B) = \tau^A \otimes \sigma^B. \quad (4)$$

Here we have written $\sigma^A$ (resp. $\sigma^B$) for operators in $\mathcal{B}(\mathcal{H}^A)$ (resp. $\mathcal{B}(\mathcal{H}^B)$). In terms of partial traces, Eq. (4) can be equivalently phrased as,

$$(\mathrm{Tr}_A \circ \mathcal{E})(\sigma) = \mathrm{Tr}_A(\sigma), \quad \forall \sigma = \sigma^A \otimes \sigma^B. \quad (5)$$

Thus, to be precise, $B$ is said to encode a *noiseless subsystem* (or *decoherence-free subspace* in the case $\dim \mathcal{H}^A = 1$) for $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ when Eq. (4) is satisfied.

The basic questions we address are the following: (1) Is there a structure theory for such subsystems? (2) If so, can it be applied to derive a canonical method to find such subsystems for arbitrary quantum operations? Our answer to the first question is yes, and for the second we make a proposal that lends itself to the possibility of a computational algorithm.

*Structure Theorem.* — Let $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ be a quantum operation. We shall write $\mathcal{E} = \{E_a\}$ when an error model for $\mathcal{E}$ is known; i.e., the operation elements $E_a$ determine $\mathcal{E}$ through the familiar operator-sum representation $\mathcal{E}(\sigma) = \sum_a E_a \sigma E_a^\dagger$ [20, 21].

The (full) *noise commutant* $\mathcal{A}'$ for $\mathcal{E}$ is the set of all operators in $\mathcal{B}(\mathcal{H})$ that commute with the operators $E_a$ and $E_a^\dagger$. The $\dagger$-algebra $\mathcal{A}$ generated by the $E_a$ is called the *interaction algebra* associated with $\mathcal{E}$. In the unital case ($\mathcal{E}(\mathbb{1}) = \mathbb{1}$) it is obvious that every $\sigma \in \mathcal{A}'$ satisfies $\mathcal{E}(\sigma) = \sigma$, and, in fact, every operator that is fixed by $\mathcal{E}$ belongs to $\mathcal{A}'$ [22]. Of course, in the general case the operator $\mathcal{E}(\mathbb{1})$ may not be so well behaved, and all that can be said for operators $\sigma \in \mathcal{A}'$ is that they satisfy $\mathcal{E}(\sigma) = \sigma\mathcal{E}(\mathbb{1}) = \mathcal{E}(\mathbb{1})\sigma$. This equation is suggestive of the more general phenomena that must be analyzed to obtain NS for arbitrary quantum operations. Given a projection $P$ in $\mathcal{B}(\mathcal{H})$, we shall make the natural identification of the subalgebra $P\mathcal{B}(\mathcal{H})P$ of $\mathcal{B}(\mathcal{H})$ with the algebra $\mathcal{B}(P\mathcal{H})$.

**Theorem 1** *Let $\mathcal{E} = \{E_a\}$ be a quantum operation on $\mathcal{B}(\mathcal{H})$. Suppose $P$ is a projection on $\mathcal{H}$ such that*

$$\mathcal{E}(P) = P\,\mathcal{E}(P)P. \quad (6)$$

*Then $E_a P = PE_a P$, $\forall a$. Define*

$$\mathcal{A}'_P := \{\sigma \in \mathcal{B}(P\mathcal{H}) : [\sigma, PE_aP] = 0 = [\sigma, PE_a^\dagger P]\}.$$

*and,*

$$\mathrm{Fix}_P(\mathcal{E}) := \{\sigma \in \mathcal{B}(P\mathcal{H}) : \mathcal{E}(\sigma) = \sigma\mathcal{E}(P) = \mathcal{E}(P)\sigma, \ \mathcal{E}(\sigma^\dagger\sigma) = \sigma^\dagger\mathcal{E}(P)\sigma, \ \mathcal{E}(\sigma\sigma^\dagger) = \sigma\mathcal{E}(P)\sigma^\dagger\},$$

*Then $\mathrm{Fix}_P(\mathcal{E})$ is a $\dagger$-algebra inside $\mathcal{B}(P\mathcal{H})$ that coincides with the algebra $\mathcal{A}'_P$; that is,*

$$\mathrm{Fix}_P(\mathcal{E}) = \mathcal{A}'_P. \quad (7)$$

*Proof.* Let $P$ be a projection that satisfies Eq. (6). Then

$$0 \leq P^\perp E_a P E_a^\dagger P^\perp \leq P^\perp \mathcal{E}(P) P^\perp = 0 \quad \forall a.$$

Hence $P^\perp E_a P = 0$, or equivalently $E_a P = PE_a P$, $\forall a$. Let $E_{a,P} := PE_aP = E_aP$, $\forall a$. It is clear that $\mathrm{Fix}_P(\mathcal{E})$

contains the commutant (taken inside $\mathcal{B}(P\mathcal{H})$) of the operators $\{E_{a,P}, E_{a,P}^\dagger\}$. Let $\sigma \in \mathcal{A}'_P$. We are required to show that $\sigma$ commutes with the operators $E_{a,P}$ and $E_{a,P}^\dagger$.

The properties $\mathcal{E}(\sigma) = \sigma\mathcal{E}(P) = \mathcal{E}(P)\sigma$, $\sigma = P\sigma P$ and Eq. (6) are seen through a calculation to imply that

$$\mathcal{E}(\sigma^\dagger\sigma) - \sigma^\dagger\mathcal{E}(P)\sigma = \sum_a [\sigma, E_{a,P}^\dagger]^\dagger[\sigma, E_{a,P}^\dagger] \geq 0.$$

(This inequality may be regarded as a generalization of the Schwarz inequality for completely positive maps from [24, 25].) Thus, given $\mathcal{E}(\sigma) = \sigma\mathcal{E}(P) = \mathcal{E}(P)\sigma$, and so $\mathcal{E}(\sigma^\dagger) = \mathcal{E}(\sigma)^\dagger = \sigma^\dagger\mathcal{E}(P) = \mathcal{E}(P)\sigma^\dagger$, it follows that

$$\mathcal{E}(\sigma^\dagger\sigma) = \sigma^\dagger\sigma\mathcal{E}(P) \quad \text{iff} \quad \sigma E_{a,P}^\dagger = E_{a,P}^\dagger\sigma, \;\; \forall a,$$
$$\mathcal{E}(\sigma\sigma^\dagger) = \sigma\sigma^\dagger\mathcal{E}(P) \quad \text{iff} \quad \sigma E_{a,P} = E_{a,P}\sigma, \;\; \forall a.$$

This completes the proof. □

Observe that the maximally mixed state $P = \mathbb{1}$ trivially satisfies Eq. (6), and the algebra $\mathcal{A}'_{\mathbb{1}}$ coincides with the full noise commutant $\{E_a, E_a^\dagger\}$. However, as discussed above, the operator $\mathcal{E}(\mathbb{1})$ may not have many nice properties. In general there may be other projections $P$ that support larger noiseless subsystems.

*Noiseless Subsystems.* — Let $P$ be a projection that satisfies Eq. (6). The structure theory for †-algebras [23] yields a unitary $U$ on $P\mathcal{H}$ such that

$$U\,\mathcal{A}'_P\,U^\dagger = \bigoplus_k (\mathbb{1}_{m_k} \otimes M_{n_k}), \qquad (8)$$

for a unique (up to reordering) family of positive integers $m_k, n_k \geq 1$. We have used $M_{n_k}$ to denote the operator algebra $\mathcal{B}(\mathbb{C}^{n_k})$, represented as matrices with respect to some orthonormal basis. Note that the algebra $\mathcal{A}'_P$ may be regarded as a subalgebra of $\mathcal{B}(\mathcal{H})$ simply by taking a direct sum $\mathcal{A}'_P \oplus O_{n_P}$ of $\mathcal{A}'_P$ together with the "zero algebra" $0_{n_P}$ of $n_P \times n_P$ matrices on $P^\perp\mathcal{H}$, where $n_P = \dim\mathcal{H} - \sum_k m_k n_k$.

The algebra structure Eq. (8) induces a decomposition of the subspace $P\mathcal{H}$ as

$$P\mathcal{H} = \bigoplus_k (\mathcal{H}^{A_k} \otimes \mathcal{H}^{B_k}), \qquad (9)$$

where $\dim(\mathcal{H}^{A_k}) = m_k$ and $\dim(\mathcal{H}^{B_k}) = n_k$. Observe that the positive operator $\mathcal{E}(P)$ belongs to the commutant inside $\mathcal{B}(P\mathcal{H})$ of $\mathcal{A}'_P$ by definition. As this commutant has structure $\mathcal{A}_P := \mathcal{A}''_P = \oplus_k(M_{m_k} \otimes \mathbb{1}_{n_k})$, it follows that there are operators $\sigma_k \in \mathcal{B}(\mathcal{H}^{A_k}) = M_{m_k}$ such that $\mathcal{E}(P) = \sum_k \sigma_k \otimes \mathbb{1}_{n_k}$.

Now let $\rho = \mathbb{1}^{A_k} \otimes \rho^{B_k}$ belong to the subalgebra $\mathbb{1}^{A_k} \otimes \mathcal{B}(\mathcal{H}^{B_k})$ of $\mathcal{A}'_P = \oplus_k(\mathbb{1}^{A_k} \otimes \mathcal{B}(\mathcal{H}^{B_k}))$. Then we have

$$\mathcal{E}(\mathbb{1}^{A_k} \otimes \rho^{B_k}) = \mathcal{E}(\rho) = \rho\,\mathcal{E}(P) = \sigma_k \otimes \rho^{B_k}. \qquad (10)$$

But Eq. (4) holds if and only if it holds for $\sigma^A = \mathbb{1}^A$ [16, 17]. Therefore, it follows from Eq. (10) that each of the subsystems $\mathcal{H}^{B_k}$ is noiseless for $\mathcal{E}$ and the following result is established.

**Theorem 2** *Let $\mathcal{E}$ be a quantum operation on $\mathcal{B}(\mathcal{H})$. Let $P$ be a projection on $\mathcal{H}$ that satisfies Eq. (6) and let $P\mathcal{H} = \bigoplus_k(\mathcal{H}^{A_k} \otimes \mathcal{H}^{B_k})$ be the decomposition of $P\mathcal{H}$ induced by the †-algebra structure of $\mathcal{A}'_P = \mathrm{Fix}_P(\mathcal{E})$. Then the subsystems $\mathcal{H}^{B_k}$, with $\dim\mathcal{H}^{B_k} > 1$, are each noiseless subsystems for $\mathcal{E}$.*

In fact, it follows that if the input states are restricted to the subspace $\mathcal{H}^{A_k} \otimes \mathcal{H}^{B_k}$, then the corresponding restriction of $\mathcal{E}$ satisfies $\mathcal{E}(P_k(\cdot)P_k) = \mathcal{E}_k \otimes \mathrm{id}_{B_k}$ where $P_k$ is the projection of $\mathcal{H}$ onto $\mathcal{H}^{A_k} \otimes \mathcal{H}^{B_k}$, $\mathcal{E}_k$ is a quantum operation on $\mathcal{B}(\mathcal{H}^{A_k})$, and $\mathrm{id}_{B_k}$ is the identity channel on $\mathcal{B}(\mathcal{H}^{B_k})$.

The NS structure for a number of unital channels have been analyzed in detail. An extensively studied class of channels arise from "collective noise", which has a number of physical interpretations (see [26, 27] for a detailed analysis of this and related NS structures). We note a connection with [28] which includes a decomposition for collective noise channels of the form $\mathcal{E} = \sum_k(\mathcal{D}_k \otimes \mathrm{id}_k)(P_k\sigma P_k)$, where the $P_k$ are projections associated with a decomposition of the system Hilbert space induced by underlying representation theory and the $\mathcal{D}_k$ are depolarizing channels (see Eq. (22) of [28]). Interestingly, this may now be seen as a special case of the general form derived here.

Let us return to the non-unital example discussed in the Introduction. A computation shows in this case that the full noise commutant satisfies $\mathcal{A}'_{\mathbb{1}} = \{E_0, E_1, E_2\}' \cong \mathbb{1}_2 \otimes M_2$, and thus supports a single qubit NS. Indeed, if $\sigma \in \mathcal{A}'_{\mathbb{1}}$ is written as $\mathbb{1}_2 \otimes \sigma_0$, $\sigma_0 \in M_2$, with respect to this unitary equivalence, then a calculation shows that

$$\mathcal{E}(\sigma) = \mathcal{E}(\mathbb{1}_2 \otimes \sigma_0) = \left(\begin{smallmatrix} 1-q & 0 \\ 0 & 1+q \end{smallmatrix}\right) \otimes \sigma_0.$$

But recall that the projection $P = |01\rangle\langle 01| + |10\rangle\langle 10|$ defines a DFS for $\mathcal{E}$; specifically, $\mathcal{E}(\sigma) = \sigma$, $\forall\sigma = P\sigma P$. Now we can see precisely how this DFS arises. Namely, $\mathcal{E}(P) = P$ satisfies Eq. (6) and thus we find a single qubit NS for $\mathcal{E}$, with $|\psi\rangle := |01\rangle$ and $|\phi\rangle := |10\rangle$, given by

$$\mathcal{A}'_P = \mathrm{span}\left\{|\psi\rangle\langle\psi|, |\psi\rangle\langle\phi|, |\phi\rangle\langle\psi|, |\phi\rangle\langle\phi|\right\} \cong M_2.$$

Notice that $\mathcal{A}'_P$ is not contained in $\mathcal{A}'_{\mathbb{1}}$, and thus this DFS would not be detected through an analysis of the full noise commutant alone. Further, while $\mathcal{A}'_{\mathbb{1}}$ and $\mathcal{A}'_P$ have the same "size" from an encoding viewpoint (i.e., a single qubit) [29], it is perhaps more convenient to work with $\mathcal{A}'_P \cong M_2$, as it can be more easily isolated within the full system Hilbert space.

In fact, this example gives an indication as to how active and passive techniques for quantum error correction can be combined to combat noise. Indeed, we have just noted that the subspace $\{|01\rangle, |10\rangle\}$ determines a DFS for $\mathcal{E}$. On the other hand, in [19] it was shown that active error correction may be used to overcome corruption by $\mathcal{E}$ of the code subspace $\{|00\rangle, |11\rangle\}$.

*Optimality of the Method.* — The previous two sections yield a canonical method to compute noiseless subsystems for a given quantum operation $\mathcal{E}$ which can be succinctly stated as follows:

(i) Compute the projections $P$ such that Eq. (6) holds.

(ii) Compute the structure of the algebras $\mathcal{A}'_P = \mathrm{Fix}_P(\mathcal{E})$ as in Eq. (8).

Then, in the notation above, the subspaces $\mathcal{H}^{B_k}$, with $\dim \mathcal{H}^{B_k} > 1$, encode noiseless subsystems for $\mathcal{E}$ via the operator algebras $\mathbb{1}^{A_k} \otimes \mathcal{B}(\mathcal{H}^{B_k})$

A crucial final step in the process is to determine if this scheme captures all noiseless subsystems for $\mathcal{E}$. We next show that this is indeed the case.

**Theorem 3** *Let $\mathcal{E}$ be a quantum operation on $\mathcal{B}(\mathcal{H})$. Suppose that $\mathcal{H} = (\mathcal{H}^A \otimes \mathcal{H}^B) \oplus \mathcal{K}$ and that $\mathcal{H}^B$ is a noiseless subsystem for $\mathcal{E}$ as in Eq. (4). Let $P$ be the projection of $\mathcal{H}$ onto $\mathcal{H}^A \otimes \mathcal{H}^B$. Then $\mathcal{E}(P) = P\mathcal{E}(P)P$ and the algebra $\mathcal{A}'_P$ contains $\mathbb{1}^A \otimes \mathcal{B}(\mathcal{H}^B)$ as a simple, unital $\dagger$-subalgebra.*

*Proof.* Let $\{|\alpha_k\rangle\}$ be an orthonormal basis for $\mathcal{H}^A$, and let $\{P_{kl} = |\alpha_k\rangle\langle\alpha_l| \otimes \mathbb{1}^B\}$ be the corresponding matrix units inside $\mathcal{B}(\mathcal{H}^A) \otimes \mathbb{1}^B$. It was proved in [16, 17] that $\mathcal{H}^B$ is noiseless for $\mathcal{E} = \{E_a\}$ as in Eq. (4) precisely when $E_a P = P E_a P$ and there are scalars $\{\lambda_{akl}\}$ such that

$$P_{kk} E_a P_{ll} = \lambda_{akl} P_{kl} \quad \forall\, a, k, l. \tag{11}$$

Note that the projection $P$ is given by $P = \sum_k P_k$, where we have written $P_k$ for $P_{kk}$. Thus we have

$$\begin{aligned} \mathcal{E}(P) &= \sum_{a,k} E_a P_k E_a^\dagger = \sum_{a,k,l,l'} P_l E_a P_k E_a^\dagger P_{l'} \\ &= \sum_{a,k,l,l'} \lambda_{alk} \overline{\lambda}_{al'k} P_{lk} P_{kl'} = \sum_{a,k,l,l'} \lambda_{alk} \overline{\lambda}_{al'k} P_{ll'}. \end{aligned}$$

Let $\sigma = \mathbb{1}^A \otimes \sigma^B \in \mathbb{1}^A \otimes \mathcal{B}(\mathcal{H}^B)$. Then since the $P_{kl}$ commute with $\sigma = P\sigma P$ we have

$$\begin{aligned} \mathcal{E}(\sigma) &= \mathcal{E}(P\sigma P) = P\mathcal{E}(P\sigma P)P \\ &= \sum_{a,k,k',l,l'} P_k E_a P_{k'} \sigma P_{l'} E_a^\dagger P_l \\ &= \sum_{a,k,k',l,l'} \lambda_{akk'} \overline{\lambda}_{all'} P_{kk'} \sigma P_{l'l} \\ &= \sigma \mathcal{E}(P) = \mathcal{E}(P)\sigma. \end{aligned}$$

In particular, this implies (with $\sigma^B = \mathbb{1}^B$) that $\mathcal{E}(P) = P\mathcal{E}(P)P$ and that the algebra $\mathbb{1}^A \otimes \mathcal{B}(\mathcal{H}^B)$ is contained in $\mathcal{A}'_P$. It is clear that $\mathcal{A}'_P$ and $\mathbb{1}^A \otimes \mathcal{B}(\mathcal{H}^B)$ have the same unit $P$, and that $\mathbb{1}^A \otimes \mathcal{B}(\mathcal{H}^B)$ is a simple (i.e., contains no non-trivial ideals) $\dagger$-subalgebra of $\mathcal{A}'_P$. □

We finish with a consequence for the unital case. The class of unital channels includes numerous physical error models such as collective noise, randomized unitary channels, etc. It is important to note that the full noise commutant captures all NS in this case. In particular, this means algebras $\mathcal{A}'_P$ may not be contained inside $\mathcal{A}'_{\mathbb{1}}$ only in the non-unital case.

**Corollary 1** *Let $\mathcal{E}$ be a unital quantum operation on $\mathcal{B}(\mathcal{H})$. If $\mathfrak{A} = \mathbb{1}^A \otimes \mathcal{B}(\mathcal{H}^B)$ is the algebra determined by a noiseless subsystem for $\mathcal{E}$ as in Eq. (4), then $\mathfrak{A}$ is a subalgebra of the full noise commutant $\mathcal{A}'_{\mathbb{1}}$.*

*Proof.* Let $P$ be the projection of $\mathcal{H}$ onto $\mathcal{H}^A \otimes \mathcal{H}^B$. By Eq. (4), there is a $\tau^A$ such that $\mathcal{E}(P) = \mathcal{E}(\mathbb{1}^A \otimes \mathbb{1}^B) = \tau^A \otimes \mathbb{1}^B$. Since $\mathcal{E}$ is a unital completely positive map, we know that $\tau^A$ is a contraction operator, and hence $\mathcal{E}(P) \leq P$. Then in fact $\mathcal{E}(P) = P$ by Lemma 2.3 from [22]. Thus, it follows from Theorem 3, and the definition of $\mathcal{A}'_P$, that $\mathfrak{A} \subseteq \mathcal{A}'_P$ is a subalgebra of $\mathrm{Fix}\,(\mathcal{E})$. □

*Conclusion.* — We have derived a structure theory for decoherence-free subspaces and noiseless subsystems that applies to arbitrary quantum operations. As an application, we have proposed a method to compute NS for any given operation. We expect that the method could be formalized into a computational algorithm, as suggested by recent literature [30, 31] which includes algorithms written to calculate operator algebra structures, but there are still details to work through. We plan to undertake this investigation elsewhere.

We discussed a non-unital example in which the maximally mixed state and a smaller projection support different single qubit noiseless subsystems. We suggest that this work motivates reconsideration of the quantum channels that appear in the literature, for the possible existence of noiseless subsystems. We wonder about possible experimental implications of this work. It would also be interesting to investigate connections with other recent noiseless subsystem related efforts such as [14, 15, 32].

*Acknowledgements.* We thank Dietmar Bisch for asking a question that partly motivated this work. We are grateful to John Holbrook, Raymond Laflamme, Rob Spekkens, and Karol Zyczkowski for helpful comments. D.W.K. would also like to thank other colleagues at UofG, IQC and Perimeter Institute for interesting discussions. This work was partially supported by NSERC.

[1] G.M. Palma, K.-A. Suominen, A. Ekert, Proc. Royal Soc. A **452**, 567 (1996).
[2] L.-M. Duan, G.-C. Guo, Phys. Rev. Lett. **79**, 1953 (1997).
[3] P. Zanardi, M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).
[4] D.A. Lidar, I.L. Chuang, K.B. Whaley, Phys. Rev. Lett. **81**, 2594 (1998).
[5] E. Knill, R. Laflamme, L. Viola, Phys. Rev. Lett. **84**, 2525 (2000).
[6] P. Zanardi, Phys. Rev. A **63**, 12301 (2001).
[7] J. Kempe, D. Bacon, D. A. Lidar, K. B. Whaley, Phys. Rev. A **63**, 42307 (2001).

[8] P. G. Kwiat, et al., Science **290**, 498 (2000).
[9] D. Kielpinski, et al., Science **291**, 1013 (2001).
[10] E. M. Fortunato, et al., New J. Phys. **4**, 5 (2002).
[11] L. Viola, et al., Science **293**, 2059 (2003).
[12] J. -C. Boileau, et al., Phys. Rev. Lett. **92**, 17901 (2004).
[13] S. D. Bartlett, T. Rudolph, R. W. Spekkens, Phys. Rev. Lett.,**91**, 027901 (2003).
[14] O. Dreyer, F. Markopoulou, L. Smolin, arxiv.org/hep-th/0409056.
[15] D. W. Kribs, F. Markopoulou, arxiv.org/gr-qc/0510052.
[16] D. W. Kribs, R. Laflamme, D. Poulin, Phys. Rev. Lett.,**94**, 180501 (2005).
[17] D. W. Kribs, R. Laflamme, D. Poulin, M. Lesosky, arxiv.org/quant-ph/0504189.
[18] C. Seife, *Teaching qubits new tricks*, Science, **309**, 238 (2005).
[19] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).
[20] M. D. Choi, Lin. Alg. Appl. **10** 285-290 (1975).
[21] K. Kraus, Ann. Physics **64** 311-335 (1971).
[22] D. W. Kribs, Proc. Edin. Math. Soc. **46** 421-433(2003).
[23] K. Davidson, $C^*$*-algebras by example, Fields Institute Monographs* (Amer. Math. Soc., Providence, 1996).
[24] M. D. Choi, Illinois J. Math. **18** 565-574 (1974).
[25] C. Davis, Proc. Amer. Math. Soc. **8** 42-44 (1957).
[26] J. A. Holbrook, D. W. Kribs, R. Laflamme, D. Poulin, Integral Eqnts. & Operator Thy. **51**, 215-234 (2005).
[27] M. Junge, P. Kim, D. W. Kribs, J. Math. Phys. **46**, 022102 (2005).
[28] S. D. Bartlett, T. Rudolph, R. W. Spekkens, Phys. Rev. A **70**, 032307 (2004).
[29] G. Kuperberg, IEEE Trans. Inform. Theory **49**, 1465-1473 (2003).
[30] J. A. Holbrook, D. W. Kribs, R. Laflamme, Quantum Inf. Proc. **2**, 381 (2004).
[31] V. Zarikian, Lin. Alg. Appl., to appear .
[32] D. A. Lidar, A. Shabani, arxiv.org/quant-ph/0505051.